

# METHOD AND APPARATUS FOR PREVENTING FRAUDULENT ACCESS IN A CONDITIONAL ACCESS SYSTEM

Publication number: JP2001519980 (T)

Publication date: 2001-10-23

Inventor(s):

Applicant(s):

Classification:

- international: **H04N7/167; G06F11/10; G06Q20/00; G06T9/00; G07F7/00; G07F7/02; G07F7/08; H04H1/00; H04L9/32; H04N5/00; H04N7/16; H04N7/16; G06F11/10; G06Q20/00; G06T9/00; G07F7/00; G07F7/08; H04H1/00; H04L9/32; H04N; H04N5/00; H04N7/167; (IPC1-7): H04N7/167; H04H1/00; H04L9/32**

- European: **G06F11/10; G06Q20/00K2C; G06T9/00T; G07F7/00C; G07F7/02E; G07F7/08F2; H04N5/00M; H04N5/00M4; H04N5/00M8; H04N7/16E2; H04N7/167D**

Application number: JP19980543230T 19980319

Priority number(s): EP19970400650 19970321; WO1997EP02106 19970425; EP19970402959 19971205; WO1998EP01606 19980319

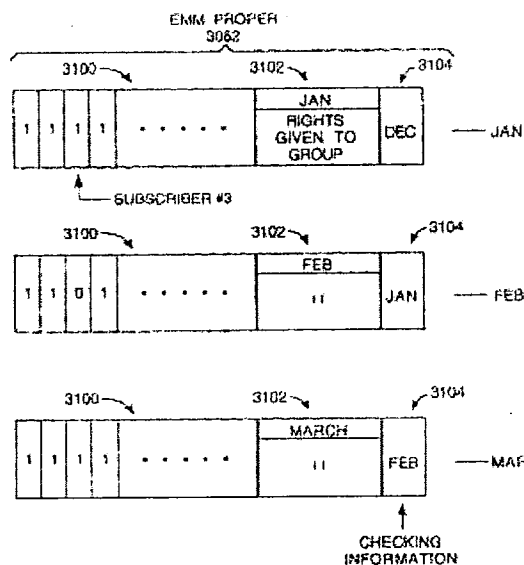
Also published as:

WO9843428 (A1)  
RU2199832 (C2)  
NO994531 (A)  
HK1025209 (A1)  
ES2185164 (T3)

Abstract not available for JP 2001519980 (T)

Abstract of corresponding document: **WO 9843428 (A1)**

A receiver/decoder is programmed only to accept a current entitlement control message (EMM) if it has received at least a previous EMM of a previous calendar period. When this is received, it is used to check present rights in the receiver/decoder. The invention prevents an original subscriber from fraudulently obtaining rights by disconnecting a decoder (before an authorising message can update the decoder's memory to prevent decryption) and by reconnecting the decoder (so as to be mistaken for a new subscriber legitimately having those rights).



(51)Int.Cl. <sup>3</sup>	識別記号	F I	テグコード (参考)
H 0 4 N 7/167		H 0 4 H 1/00	E
H 0 4 H 1/00		H 0 4 N 7/167	Z
H 0 4 L 9/32		H 0 4 L 9/00	6 7 1

審査請求 未請求 予備審査請求 有 (全 30 頁)

(21) 出願番号 特願平10-543230  
 (86) (22) 出願日 平成10年3月19日 (1998. 3. 19)  
 (85) 翻訳文提出日 平成11年9月17日 (1999. 9. 17)  
 (86) 国際出願番号 PCT/EP 98/01606  
 (87) 国際公開番号 WO 98/43428  
 (87) 国際公開日 平成10年10月1日 (1998. 10. 1)  
 (31) 優先権主張番号 97400650. 4  
 (32) 優先日 平成9年3月21日 (1997. 3. 21)  
 (33) 優先権主張国 ヨーロッパ特許庁 (E P)  
 (31) 優先権主張番号 PCT/EP 97/02106  
 (32) 優先日 平成9年4月25日 (1997. 4. 25)  
 (33) 優先権主張国 世界知的所有権機関 (W O)

(71) 出願人 カナル プラス ソシエテ アノニム  
 フランス国 エフー75711 パリ セデッ  
 クス 15 クアイ アンドレ シトロエン  
 85/89  
 (72) 発明者 メイラード, マイケル  
 フランス国 エフー28130 マインテノン  
 アベニュー デュ マレシャル レセル  
 42  
 (74) 代理人 弁理士 齊藤 武彦 (外1名)

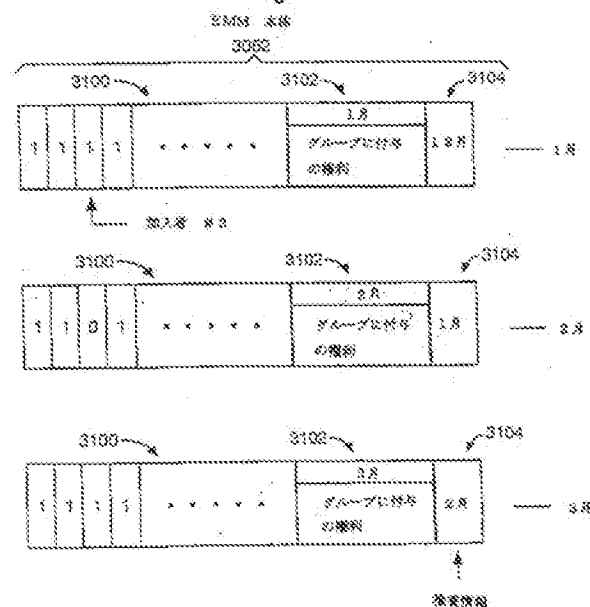
最終頁に続く

(54) 【発明の名称】 条件付きアクセスシステムにおける不正なアクセスを防止する方法および装置

## (57) 【要約】

レシーバー/デコーダーは、少なくとも前のカレンダー期間における前の EMM (エンタイトルメント・コントロール・メッセージ) を受信したら、現 EMM を受け入れるためにのみプログラムされる。これが受信されると、レシーバー/デコーダーの現在の権利を検査するために使用される。この発明は、原加入者が、(公認メッセージが暗号解読を防止するためデコーダーのメモリを更新できる前に) デコーダーを切断することにより、また(合法的に権利を有する新加入者と間違えられるように) デコーダーを再接続することによって不正に権利を取得されないようにする。

Fig.5.



【特許請求の範囲】

1. 加入者群のためのエンタイトルメント・マネージメント・メッセージ (EMM) を受信するため加入者のレシーバー／デコーダーに連結される条件付きアクセスシステムにおける不正なアクセスを防止する方法であって、前記システムをそれぞれ加入者にアクセスさせ得るようにした方法において、  
少なくとも先のカレンダー期間の先のEMMを受信したならば現在のカレンダー期間の現在のEMMのみを受け入れるレシーバー／デコーダーをプログラムする工程を具備する不正なアクセスを防止する方法。
2. 現在のEMMで冗長日付情報を送信する工程、および現在のEMMを受信し冗長日付情報を使用することにより前記先行するEMMが受信されたかどうか検査する工程を更に具備する請求項1記載の方法。
3. 各EMMは、現在のアクセス権利に関する権利日付情報および先行するアクセス権利に関する対応検査日付情報を具備し、この検査日付情報は冗長日付情報を構成する請求項3記載の方法。
4. 冗長日付情報は先のカレンダー期間のECMキーである請求項2又は3に記載の方法。
5. 加入者権利は規則的時間ベースに基づいて変化し、冗長日付情報は直前の期間に関する請求項2ないし4記載の方法。
6. カレンダー期間が時間的に非隣接であり、および（または）このような期間の間にリアルタイムの不規則量が存在する前記請求項のいずれかに記載の方法。
7. 任意に加入者権利に変化があるときのみ現在のEMMに、グループにおける加入者の加入権利を表す位置を有する加入者ビットマップを選択的に具備する前記請求項のいずれかに記載の方法。
8. 加入者群のためのエンタイトルメント・マネージメント・メッセージ (EMM) を受信するため加入者のレシーバー／デコーダーに連結される条件付きアクセスシステムにおける不正なアクセスを防止する方法であり、前記システムをそれぞれの加入者にアクセスさせ得るようにした方法に使用されるトランスミッタであって、該レシーバー／デコーダーは、もし少なくとも先のカレンダー

- 一期間の先の EMM を受信したら、現在のカレンダー期間の現在の EMM を受け入れるためにのみプログラムされるようになっている該トランスミッタは、
- 冗長日付情報をレシーバー/デコーダーが使用して前記先の EMM が受信されたかどうかを検査できるように、現在のカレンダー期間の現在の EMM で冗長日付情報を送信する手段を具備するトランスミッタ。
9. 各 EMM は、アクセスの現在の権利に関する権利日付情報と、アクセスの先の権利に関する対応検査日付情報とを具備し、このような検査日付情報は冗長日付情報を構成する請求項 8 記載のトランスミッタ。
10. 冗長日付情報は先のカレンダー期間の ECM キーである請求項 8 または 9 記載のトランスミッタ。
11. 条件付きアクセスシステムにおける不正アクセスを防止する方法に使用されるレシーバー/デコーダーであって、該レシーバー/デコーダーは条件付きアクセスシステムに連結され、加入者群のためエンタイトルメント・マネージメント・メッセージ (EMM) を受信するために設けられ、前記システムをそれぞれの加入者にアクセス可能とするレシーバー/デコーダーにおいて、
- 少なくとも先のカレンダー期間の先の EMM を受信したのならば、現在のカレンダー期間の現在の EMM を受け入れるためにのみプログラムされる手段を具備するレシーバー/デコーダー。
12. 前記手段は、前記先の EMM が現在の EMM に含まれる冗長日付情報を使用して受信されたかどうかを検査するためにプログラムされる、請求項 11 記載のレシーバー/デコーダー。
13. 各 EMM は、アクセスの現在権利に関する権利日付情報と、アクセスの先の権利に関する対応検査日付情報とを具備し、このような検査日付情報は冗長日付情報を構成する請求項 12 記載のレシーバー/デコーダー。
14. 冗長日付情報は先のカレンダー期間の ECM キーである請求項 12 または 13 記載のレシーバー/デコーダー。
15. 添付図面を参照し本文に実質的に記載される不正なアクセスを防止する方法。
16. 添付図面を参照しかつ該図面に例示されて本文に実質的に記載されるトラン

スミッタ。

17. 添付図面を参照して本文に実質的に記載されるレーザー／デコーダー。

#### 【発明の詳細な説明】

条件付きアクセスシステムにおける不正なアクセスを防止する方法および装置  
産業上の利用分野

本発明は、加入者のレシーバー／デコーダーに連結される条件付きアクセス・システムにおける不正なアクセスを防止する方法および装置に関する。この技術は送信された暗号化データをたとえば、公認加入者のレシーバー／デコーダーにより受信し及び暗号解読するデータ通信分野に使用される。

ここで使用される用語「レシーバー／デコーダー」とは、符号化または非符号化信号、たとえば、テレビおよび／またはラジオの信号を受信するレシーバーをいう。この用語はまた、受信信号を復号化するデコーダーをいう。このようなレシーバー／デコーダーの実施例は、たとえば、“セット・トップ・ボックス”において受信信号を復号化するレシーバーと一体のデコーダーまたは、物理的に分離されたレシーバーと結合して機能するデコーダーを含む。

このレシーバー／デコーダーは、上記では条件付きアクセス・システム“に連結”されたものとして記載されており、これはレシーバー／デコーダーが条件付きアクセス・システムの一部を形成するかまたはそこから分離されているかのいずれかの可能性を含んでいる。

排他的ではないが、特に、本発明は、下記の好ましい特徴のいくつかまたはすべてを有する大量市場向けの放送システムに使用される。これは、情報放送システム、好ましくはラジオおよび／またはテレビ放送システムでもよい；これは、（ケーブルまたは地球送信にも適用できるが）衛星システムでもよい；これは、好ましくは、MPEG、さらに好ましくは、MPEG-2であってデータ／信号送信用圧縮システムを使用するデジタルシステムでもよい。

これは、対話方式の可能性が得られる。および、これは、スマートカードも使用できる。再び言う、本発明はデジタルオーディオ可復的送信システムに関連して使用されるものである。本発明に関連して、用語“デジタル・オーディ

オ・可復送信システム”は、主としてオーディオの可復またはマルチメディアのデジタルデータを送信または放送するすべての送信システムをいう。本発明は

特に、ディジタルテレビジョンシステムの放送に適用できるけれども、本発明は、マルチメディア・インターネット応用などの固定電気通信網から送られるデータをろ致する際にも同等に使用される。

ここで使用されるように、用語“スマートカード”は、排他的でないが、たとえば、マイクロプロセッサおよび（または）メモリ格納作用を持つチップベースカード装置を含む。また、この用語には、他の物理的型式、たとえば、TVデコーダシステムによく使用されるようなキー形状装置、を有するチップ装置も含まれる。

用語MPEGは、インターナショナル・スタンダード・オーガニゼーションの作業グループ“モーション・ピクチャ・エキスパート・グループ”により開発されたデータ伝送基準、とくに、排他的でないが、ディジタルテレビジョン応用に開発され、書部ISO13818-1、ISO13818-2、ISO13818-3、およびISO13818-4に記載されるMPEG-2基準をいう。本願のコンテキストにおいて、用語は、ディジタル・データ送信分野に適用できるMPEGフォーマットのすべての変形、修正または開発を含む。

本発明の目的は、データを、たとえば、安全性の面から受信権を有する加入者その他購入者に提供するため使用できる、データ通信方法、トランスミッター、およびレシーバー／デコーダーを提供することにある。

#### 従来技術

既存の放送システムでは、受信権を得るためスマートカードが加入者により使用され、本発明によれば、カードを悪用してカードの所有者の権利に対して詐欺行為を行うことを防止しなければならぬという問題があることが見出された。

たとえば、周知のMPEGテレビジョン加入者システムでは、異なる加入者または加入者群の権利が、たとえば、月別で集中的に検査可能であり、許可メッセージがその後、中央局から各加入者または加入者群に送られて権利の使用を認可

（または阻止）する。許可メッセージは、毎月それぞれ加入者本人に割り当てられるものであり、異なるビットマップ位置にある単に“1”または“0”であり、“1”のみがそれぞれビットマップ位置の加入者に権利の使用を許可し、“0

”はその権利の使用を否定する。

このシステムについてつぎの問題が本発明により確認されている。たとえば、もし原加入者が、権利に対する支払いを停止すれば、一定期間経過後には、システムは最早、以前に割り当てたビットマップ位置の原加入者を確認しなくなり、それからこの位置は“新たな”加入者の確認に割り当てられる。新たな加入者が支払いをして、権利の使用を許可されれば、再びビットマップ位置で“1”となる。もし、“原”加入者のレシーバー／デコーダーにおいて、次の許可メッセージが（“原加入者”に連動する）リンク条件付きアクセスシステムを更新する前にデコーダーが切斷されれば、またデコーダーが後で再接続されれば（またはクロックがリセットされれば），“原”加入者は、権利の使用を許可されていた“新たな”加入者と間違えられて、“原”加入者はそれにより不正に権利を得ることになる。

本発明は、この問題を解決するものであり又加入者の権利が典型的ではあるが排他的でなく、精算に左右される期間中認可される他の同様な、またはこれに関連する諸問題を解決しようとするものである。たとえば、異なる加入者が確実な区域にアクセスし、または情報を確保し、または何等かの他の確実なサービスを確保するためにシステムを使用することが許可されるというような支払い以外の事項に対し権利は認可され得るものである。

#### 発明の開示

本発明に関連して、用語“EMM”および“ECM”が使用される。

エンタイトルメント・マネージメント・メッセージ即ちEMMは、1人の加入者または加入者群に指定されたメッセージである。EMMは普通、署名認可システムにより発生し、MPEG-2の流れで多重化される。普通、たとえばグループ使用のための所謂“マネージメント”キーで暗号化される。従って、それは加

入者群のすべての加入者に共通なキーにより暗号化される。

エンタイトルメント・コントロール・メッセージすなわちECMは、1つのスクランブルで処理して送られるメッセージである。ECMは使用者に、制御語を反スクランブル化して復元させることを可能となしそれによってテレビジョン（



または同様な）プログラムを反スクランブル化して復元を可能とする権利を得るものである。キー（ここで“ECMキー”という）は、加入者が使用するスマートカードはECMを解読するのにECMキーを必要とするため、EMMを介し加入者に送られる。解読されたECMは制御語を反スクランブル化して復元、従ってプログラムを復元するのに使用される。

本発明の一態様によれば、加入者群のためのエンタイトルメント・マネージメント・メッセージ（EMM）を受信するため加入者のレシーバー／デコーダーに連結される条件付きアクセスシステムにおける不正なアクセスを防止する方法であり、前記システムをそれぞれ加入者にアクセス可能にした方法であって、前記方法は：

少なくとも先のカレンダー期間中における先のEMMを受信したならば現在のカレンダー期間の現在のEMMを受信するレシーバー／デコーダーのみをプログラムする工程；を具備するものである。

従って、不正なアクセスを防止する問題は解決される。

この方法は、さらに「現在のEMMで冗長日付情報を送信する工程、および現在のEMMを受信し冗長日付情報を使用して前記先のEMMが受信されたかどうか検査する工程」を具備することが好ましい：

第一の好適な実施例において、各EMMは、現在のアクセス権利に関する権利日付情報および先のアクセス権利に関する対応検査日付情報を含み、この検査日付情報は冗長日付情報を構成する。これは本発明を実施する特に効果的な方法である。

第二の好適な実施例において、冗長日付情報は先のカレンダー期間のECMキーである。これはこのような情報を表すのに都合のよい他の方法である。

加入者権利は規則的時間ベースで変化し、冗長日付情報は直前期間に関する。レシーバー／デコーダーが放送システムにおける複数のレシーバー／デコー

ダーの一つであるという本発明の一つの図示例において、加入者は、プログラムを受信する権利に対し現在の月に支払わねばならず、加入者の権利は（支払わないものもあるから）月ベースで変化するべきである。そこでビットマップを使用し

て現在の月の権利を指示するのが例である。この場合、現在のEMMがデコーダーにより受信されると、冗長日付情報、たとえば、“先の”ECMキーは直前の月のものであると考えられる。しかし、順次期間にする必要がないのは、“現在”と“先の”期間が時間が非隣接であり、このような期間間のリアルタイムは不規則量となるからである。それでも、典型的には、先のEMMは直前のカレンダー期間であり、期間は順次である。

加入者権利に変化があるとき、現在のEMMにおいて、グループにおける加入者の加入権利を表す位置を有する加入者ビットマップを含むのが好ましい。しかし、これは、すべての加入者が許可されている場合、たとえば、すべての加入者がそれぞれカレンダー期間の予約料を支払った場合には不要であり、したがって、これは加入者権利に変化があるときにのみ生ずる。

本発明の他の態様によれば、加入者群のためのエンタイトルメント・マネージメント・メッセージ（EMM）を受信するため加入者のレシーバー／デコーダーに連結される条件付きアクセスシステムにおける不正なアクセスを防止する方法に使用されるトランスミッタが提供されるものであり、前記トランスミッタは前記システムをそれぞれ加入者にアクセスさせ得るようになり、レシーバー／デコーダーは、もし少なくとも先のカレンダー期間の先のEMMを受信したら、現在のカレンダー期間の現在のEMMを受信するためにのみプログラムされるようになっており、該トランスミッタは：

冗長日付情報をレシーバー／デコーダーが使用して前記先のEMMが受信されているかどうかを検査できるように現在のカレンダー期間の現在のEMMで冗長日付情報を送信する手段を具備する。

各EMMは、好ましくは現在の、アクセス権利に関する権利日付情報と、先行するアクセス権利に関する対応検査日付情報とを含み、このような検査日付情報は冗長日付情報を構成する。更にまた、冗長日付情報は先行カレンダー期間のECMキーである。

本発明の他の態様によれば、条件付きアクセスシステムにおける不正アクセスを防止する方法に使用されるレシーバー／デコーダーが提供され、レシーバー／

デコーダーは条件付きアクセスシステムに連結され、加入者群のためエンタイトルメント・マネージメント・メッセージ（EMM）を受信して前記システムをそれぞれの加入者にアクセス可能とし、該レシーバー／デコーダーは、

少なくとも先行カレンダー期間の先行のEMMを受信したなら現在のカレンダー期間の現在のEMMを受け入れるためにのみプログラムされた手段を具備するものである。

前記手段は、前記先のEMMが現在のEMMに含まれる冗長日付情報を使用して受信されたかどうかを検査するためにプログラムされる。

各EMMは、アクセスの現在権利に関する権利日付情報と、アクセスの先の権利に関する対応検査日付情報とを含み、このような検査日付情報は冗長日付情報を構成する。また、冗長日付情報は先のカレンダー期間のECMキーである。

本発明は、さらに添付図面を参照しそこに例示されたように、ここに実質的に記載されるレシーバー／デコーダーを提供する。

本発明の好適な実施例は衛星テレビジョン・システムに関するが、本発明はケーブル回路網（必ずしもテレビジョン信号を扱わない）を含む他のデータ通信回路網にも適用できる。

#### 図面の簡単な説明

つぎに本発明の好適な特徴を、例示として、添付図面を参照して説明する。

図1はデジタル・テレビジョン・システムの全体構造を示す。

図2はスマートカードの全体構成を示す。

図3は条件付きアクセスシステムに使用されるエンタイトルメント・マネージメント・メッセージ（EMM）の構成を示す。

図4はグループ内のすべての加入者に共通なグループ・マネージメント・キーKgにより暗号化されるEMMの構成を示し、また既存システムが有する問題を例示する。

図5は本発明に従って暗号化されるEMMの構成の部分を示す。

図6は第一の好適な実施例を例示する。

図7は第一実施例を例示する流れ線図を示す。

図8は別の好適な実施例を例示する。

#### 実施態様の説明

図1は、圧縮デジタル信号を送信する周知のMPEG-2圧縮システムを使用する、従来のデジタル・テレビジョン・システム2000を含むデジタル放送受信システム1000を示す。放送センターにおけるMPEG-2圧縮機2002はデジタル信号流れ（典型的に、ビデオ信号の流れ）を受信する。圧縮機2002は連係部2006によりマルチプレクサーとスクランブラー2004に接続される。マルチプレクサー2004は複数の別の入力信号を受信し、1つ以上の移送流れを組立て、圧縮デジタル信号を連係部2010を介し放送センターのトランスミッター2008に送信し、これはもちろんテレコム・リンクを含み多様な型式をとることができる。トランスミッター2008は、電磁信号をアップリンク2012を介し衛星トランスポンダー2014に送信しここでそれらは電子処理され、仮想ダウンリンク2016を介し、一般にエンドユーザーの所有または賃借の皿状のアンテナ・レシーバー/デコーダー2018に放送される。レシーバー/デコーダー2018が受信した信号はエンドユーザーの所有または賃借の集積レシーバー/デコーダー2020に送信され、エンドユーザーのテレビジョンセット2022に接続される。レシーバー/デコーダー2020は圧縮MPEG-2信号をテレビジョンセット2022用のテレビジョン信号に復号化する。

条件付きアクセス・システム3000（条件付きベースでアクセス可能）はマルチプレクサー2004とレシーバー/デコーダー2020に接続され、一部は放送センター、又一部はデコーダーに位置する。エンドユーザーは一つ以上の放送サプライヤーからデジタル・テレビジョン放送にアクセスできる。商用オフア（すなわち、放送サプライヤーが販売する1つまたは複数のテレビジョン・プログラム）に関するメッセージを解釈できるスマートカードは、レシーバー/デコーダー2020に挿入できる。デコーダー2020とスマートカードを用いて、エンドユーザーは予約方式または画面単位支払（Pay-Per-View）方式でイベントを購入する。

条件付きアクセス・システム3000は加入者公認方式（SAS）を具備する。SAS方式は、（他の形式の連結も別に使用できるが）それぞれのTCP-IP連係により、1つ以上の加入者管理システム（SMS）（各放送サブライヤーにつき1つのSMS）に接続される。また、1つのSMSを2箇所の放送サブライヤーで共有してもよく、または一人のサブライヤーが2つのSMSを使用する等である。

マルチプレクサ2004とレシーバー／デコーダー2020に接続され、一部は放送センター、一部はデコーダーに位置する、対話型システム4000もまた、エンドユーザーにモデム・バック・チャンネル4002を介し種々のアプリケーションと相互交流を可能にする。

デジタル・テレビジョン・システムの構造と作用は一般に周知であるので、これ以上詳細は述べない。

ドーター型または“署名者”型のスマートカードは図2に略示され、使用時レシーバー／デコーダー3020のカードリーダー（従来の設計よりなる）における対応コンタクト配列に接続される標準コンタクト配列102に結合される入力／出力バスを有するモトローラ（Motorola）6805の如き8ビット・マイクロプロセッサ100を具備する。マイクロプロセッサ100はまた、好ましくはマスクされたROM104、RAM106およびEEPROM108に対するバス接続を備える。スマートカードは、それぞれスマートカードの物理的パラメーター、チップ上のコンタクトの位置、および外部システム（および特にレシーバー／デコーダー2020）とスマートカード間の通信を定めるISO7816-1、7816-2および7816-3標準プロトコルに従う。これについてはここでさらに述べない。マイクロプロセッサ100の1つの機能はスマートカードのメモリを管理することである。

つぎに典型的EMMの構成を図3を参照して説明する。基本的に、一連のデジタル・データビットとして実行されるEMMは、ヘッダー3060と、EMM

本体3062と、シグネチャ3064とからなる。一方ヘッダー3060は、タイプが個人、グループ、聴衆その他のタイプかを識別する型式識別子3066

と、EMMの長さを与える長さ識別子3068と、EMMの任意アドレス3070と、オペレーター識別子3072と、キー識別子3074とからなる。EMM本体3062はもちろんその型式により大きく変化する。しかし、現状ではEMMは、簡潔にいうと、所謂“グループ更新”型のEMMである。最後に、典型的に8バイト長をもつシグネチャ3064は、EMMにおける残存データを破壊しないように多数のチェックが与えられる。

本発明は主として下記の背景に関与する。

#### 発明の背景

MPEGを使用する既存の放送システムでは、月々の加入者公認（EMM）メッセージを送るのに必要な帯域幅を減少するために、グループのすべての加入者に共通なグループ管理キーK<sub>g</sub>により暗号化されたグループ更新用EMMを使用するのが通例である。図4に示すように、EMM本体は、典型的には256ビットである、加入者ビットマップ3100を備えている。ビットマップの各ビットは加入者に相当する。例示では、ビット#3は加入者#3に相当する。EMM本体はまた、その月のグループにおけるすべての加入者の予約権利を詳述する権利部3102を備え、またその月の、典型的にはつぎの月のECMキーを含む。加入者が1月分の予約料を正しく支払っていると仮定すると、この位置の正ビット1の存在は、加入者のデコーダーに（キーK<sub>g</sub>でメッセージを解読した後）、加入者は確かに、予約権利部で規定されているこのグループのプログラムを受信する資格があることを指示する。各個プログラムは、ECMキーを使用して暗号解読されたECMを効果的に使用して復元される。

加入者が2月分の必要料金を支払わなければ、ビットマップはこの位置でゼロビット0を含む。レシーバー/デコーダーのスマートカードがメッセージを復号化した後、ビット#3でゼロの存在は、デコーダーに対して、これら権利を受ける資格がないことを指示し、スマートカードはこれを表示して適切な処置をとる。実際には、関係キーを削除する命令は分離した別のEMMで送られる。

3月の月に対しては、新加入者がグループに入れられることは全く可能である。

これが全く規則的に生ずるのは、加入者グループが、グループ数および送付されるべきEMMメッセージ数を減少するため屢々再編成されるからである。この場合、新加入者にビット#3が割り当てられることになる。新加入者が彼のキーKgでメッセージを復号化すると、彼はこのグループに相当する権利を受けるべき資格を示すこの位置での正ビット1を検出する。

上記のシステムは比較的だまされやすいとされている。加入者#3の場合、2月に簡単にデコーダーを切斷できる。こうすると、2月のEMMも受けないだろうし、又関係キーを削除する命令も受けないであろう。

3月のデコーダーの再接続により、現在の不正デコーダーをして、ビット#3で（新加入者に意図される）正ビットメッセージを含み、3月のEMMを復号化させ得る。デコーダーはそれを詳細し、このグループに関連する権利を取得し続け、グループメッセージのビット#3が、新合法加入者と先の不正加入者との2つのデコーダーに権利を有効に与えるという異常事態が生ずる。

#### 登明の好適の実施例

この問題は、図5で概略図示するように各EMMと共に順次冗長検査日付情報を送信することにより解消される。各レシーバー／レコーダー2020は、少なくとも前月のEMMを受領していれば、EMMメッセージを受け入れるためにのみプログラムされる。権利は毎月変わるの、（前権利部3104に含まれるように）前権利に対し（現在の権利部分3102に含まれる）デコーダーに格納された現在の権利を検査することのみが単に必要である。

第一の好適な実施例において、図6を参照してさらに詳述すれば、レシーバー／レコーダーに格納される現在の権利は、検査日付3110形式の冗長日付情報によって前権利に対し検査される。従ってEMM本体3062は、EMMに含まれる新権利が有効になるまで、日付を表す権利日（または老朽化した日付）3112に加えて、検査日付3110を含む。検査日付は、権利日付より早い一ヶ月（または他の適当な時期）である。EMM本体もまた、1つまたは典型的にはそれ以上のECMキー3114形式の、権利それ自身を含み；少なくとも現在の月のECMキーが、実施例では、つぎの月のECMキーと同様に設けられる。

図6はまた、図2に図示されたスマートカードのEEPROM108の関係内

容を示す。これらの内容はスマートカードに格納される権利日付3116である。

グループ更新EMMが現在処理される仕方を図7の流れ線図を参照して説明する。第一工程3200で、EMMはレシーバー/レコーダー2020に受信され、関係データは、レシーバー/レコーダーに接続されかつ、本目的のためレシーバー/レコーダーの一部と考えられるスマートカードに送られる。EMMは、種々のメモリ104、106および108と共同してスマートカード・マイクロプロセッサ100により処理される。第二工程3202で、加入者ビットマップ3100は、関係加入者について検査される。ビットマップの関係箇所に“1”が現れれば、マイクロプロセッサはEMMをさらに処理する。ビットマップの関係箇所に“0”が現れれば、処理は停止される。第三工程3204で、格納権利日付3116は検査日付3110に対し検査される。検査日付が格納権利日付より少なくまたは同等であれば、処理は継続され；さもなければ処理は停止される。第四の最終工程3206で、格納権利日付3116は、マイクロプロセッサの制御の下、新たな放送権利日付3112に変更される。放送ECMキー3114はそれから適切に使用される。

つぎに図6に戻ると、第一の好適な実施例の作動は、1998年1月、2月および3月を（例として）表す3個の列を参照して後続している。まず、グループ更新EMMは、関係月中多数回放送される。1997年の12月の月では、スマートカードEEPROM108は、12月の関係ECMキーが使用できるように、31.1.98の権利日付を格納している。1月には、1月（つぎの月）ECMキーが12月EMMとともに放送され、権利日が31.1.98であると、加入者は1月EMMが首尾よく受け入れられる前でも権利を持ち続ける。1月EMMの最初の良い受け入れがあると、31.1.98の検査日付は31.1.98の格納権利日付より早いので、格納権利日付は新放送権利日付3112に変更され、その日付は28.2.98である。1月中にさらに1月EMMの受け入れがあると、図7に示す工程3200から3206までが行われるが、格納権利日付には変更がない。

2月に、一方で加入者#3がレシーバー/レコーダー2020を作動したまま



にすると、2月のEMMが受け入れられスマートカードに移るが、(図7の工程

3で)ビットマップの関係箇所の値は“0”であるから、格納権利日付に変更がなく、28. 2. 98のままである。

他方、レシーバー/レコーダー2020を不作為にしたままにすると、(理解される)幾分異なる理由であるにせよ、同様に格納権利日付には何等変更はない。

3月に、加入者ビットマップの関係箇所の値が今“1”か“0”かに関係なく格納権利日付は、31. 3. 98の検査日付は28. 2. 98の格納権利日付より後になるため、格納権利日付は再び変わらないので、加入者は、3月に使用できるECMキーを持たないことになる。そのため、権利は効果的に停止されてしまっている。事実、権利は特別の再活動EMMによって元通りにされるに過ぎない。

第一の好適な実施例に特に密接に関係すると考えられる第二の好適な実施例において、放送EMMの検査日付3110は前月のECMキーと交換され、格納権利日付3116は(つぎの月と反対の)今月のECMキーと交換される。従って、先月のECMキーは今月のメッセージで放送される。ECMキーそれ自身とECMキーと関連(およびともに放送される)する日付とで比較される。いずれの場合も、放送ECMキーは、ECMキー自身が特別の月と関連しているので、冗長日付情報を表すものと考えられる。

従って、図5を参照すると、(冗長日付情報として12月のECMキーを含む)1月のEMMを最初に受け入れる前に、スマートカードは12月のECMキーをその中に格納している。放送と格納ECMキー間の比較結果は明白であり、従って12月のECMキーは1月のECMキーに変更される。

不正加入者が2月のデコーダーを切断したとすれば、受け入れた前の権利は1月となる。3月用のEMMが到来すると、デコーダーは2月のECMキーの不在を検出して適切な動作をする。たとえば、問題点についてのシステム権限を変えて、3月の権利の移転を拒否する等のことをする。

最初の2つの好適な実施例は、スマートカードに格納される情報として、典型

的にどんな場合でも格納される情報を採用するので、特に好適である。これにより、スマートカード内の格納スペースが経済的に使用される。

第三の好適な実施例において、冗長日付情報は、一ヶ月以上の前の月の間スマ

ートカードに格納される。たとえば、直前の1ヶ月の間格納されている情報とともに、たとえば、一ヶ月または二ヶ月の前の月の間格納される。

第四の好適な実施例において、検査日付3110は適当な確認データ3110（たとえば、完全に異なる、できればランダムな検査日付その他ランダムな数）と交換され、これはそれに対応して格納権利日付3116の代わりにスマートカードに格納されるであろう。このような状況で、権利日付3112に加えて、もう1つの確認データが放送され、それは、確認データ3110と比較するためつぎの月の間スマートカードに格納され得る権利日付3112よりむしろこのデータである。

第五の好適な実施例において、冗長日付情報は放送されないで、むしろスマートカードまたはレシーバー/デコーダーが、各月のEMMが受信されているかどうかの記録を保持する。前月のEMMが受信されていなければ、上記の第一実施例どおり、さらなる今月のEMMの処理は停止される。この記録は、たとえば、表形式である。表には、各月のEMMまたはECMもしくはその一部を含むこともある。

上記の一変形として、すべての加入者が予約料を正しく払っていれば、メッセージは全く、正の1の値よりなるので、EMMとともに加入者のビットマップを送る必要はなくなる。従って、簡潔的には、ビットマップは、図8に示すように、加入者の変更のみ送られる。

なお、本発明は例示としてのみ上記説明され、詳細な変形は発明の請求範囲内であれば実施可能である。

Fig.1.

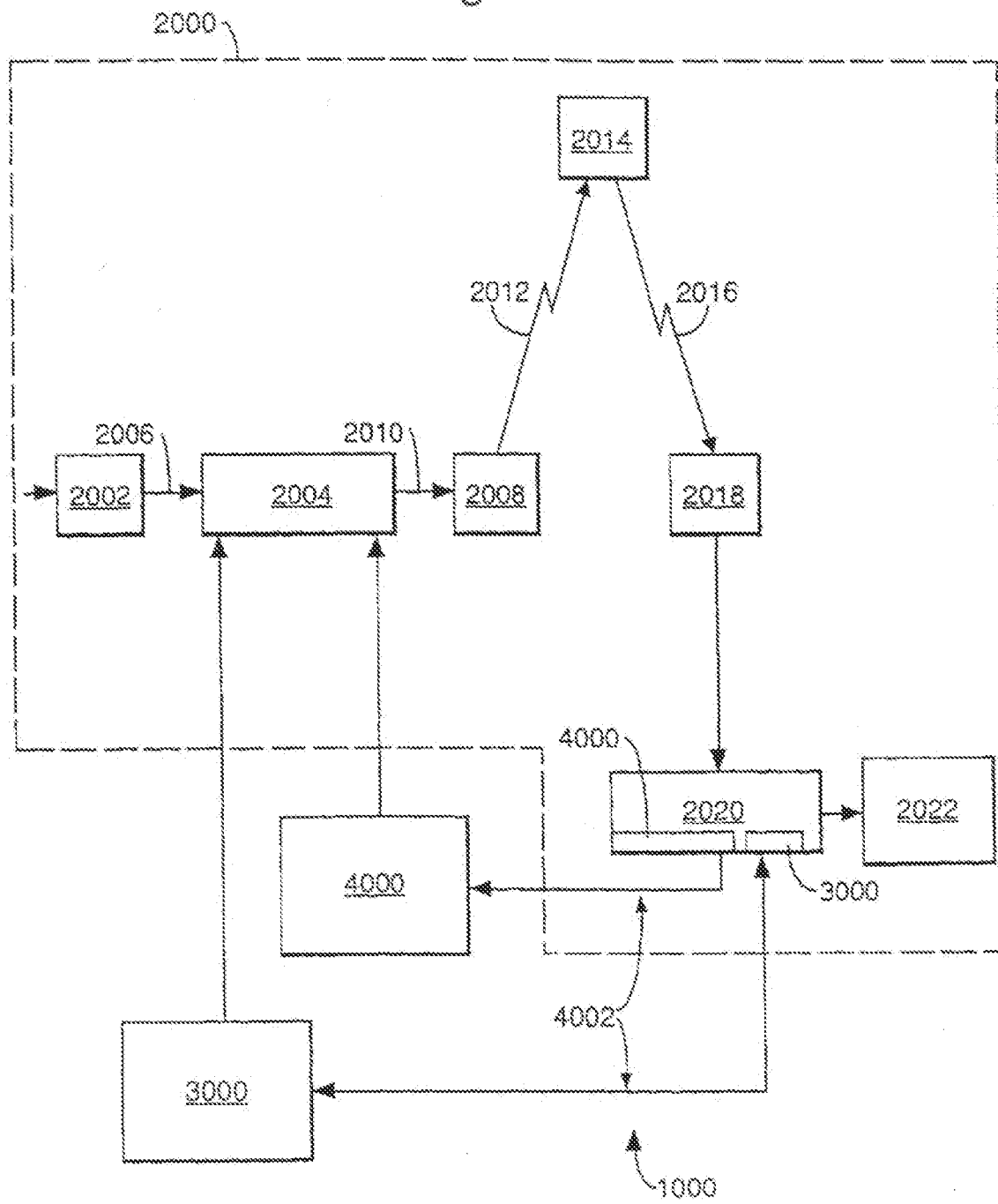


Fig.2.

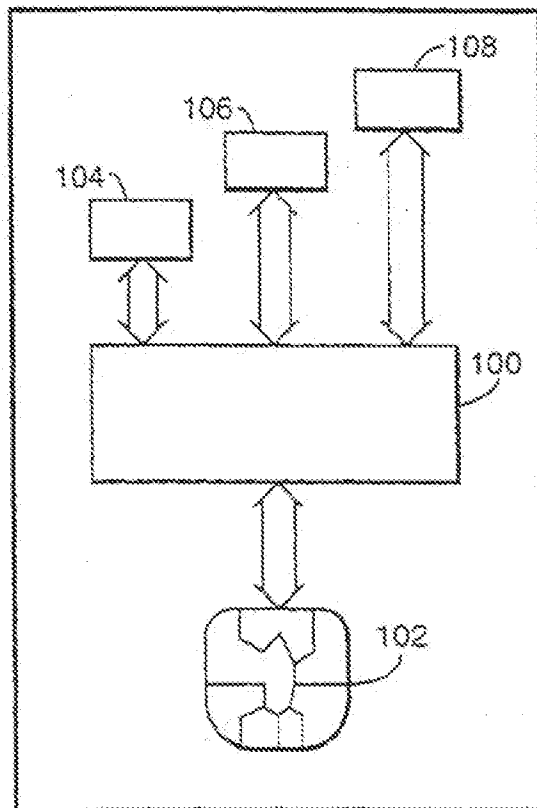


Fig.3.

3066	3068	3070	3072	3074				
型式識別子	長さ識別子	アドレス	オペレータ識別子					
ヘッダー 3050				EMM 本体 3062		シグネチャ 3064		

Fig.4.

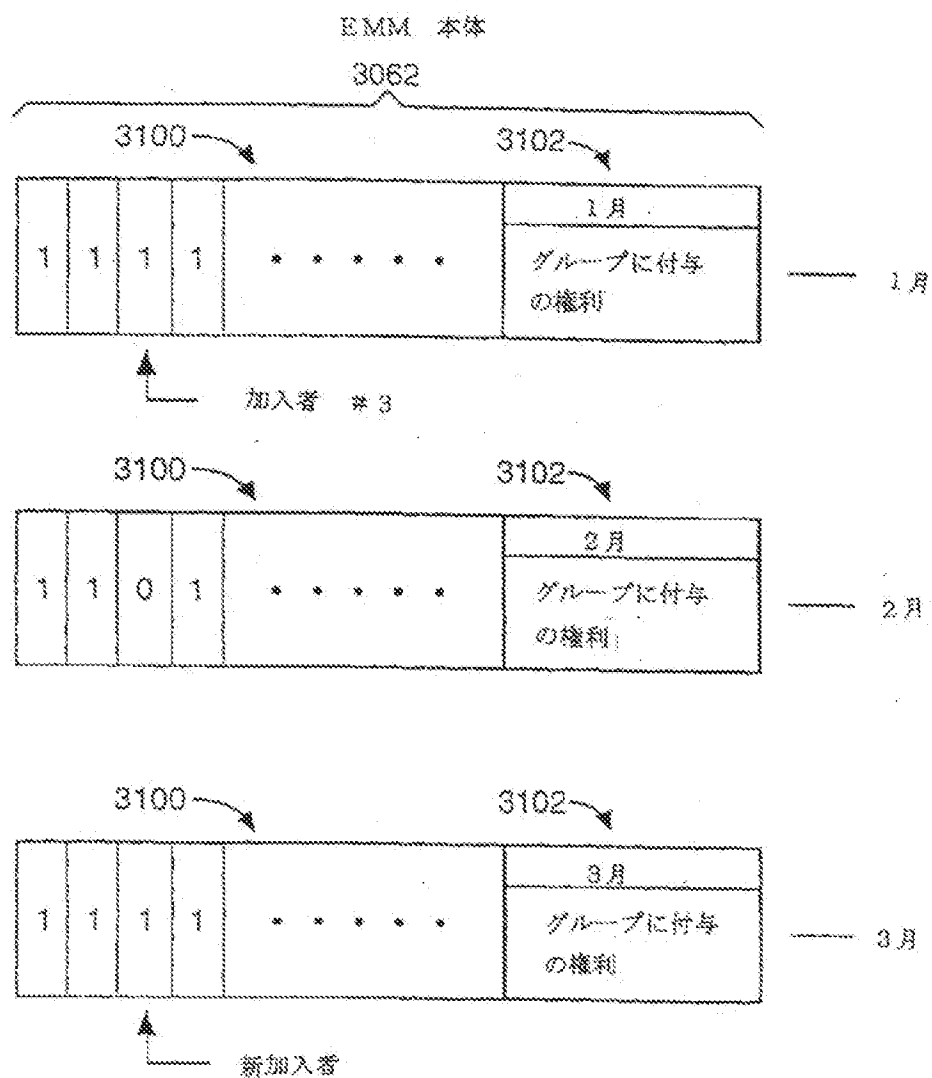


Fig.5.

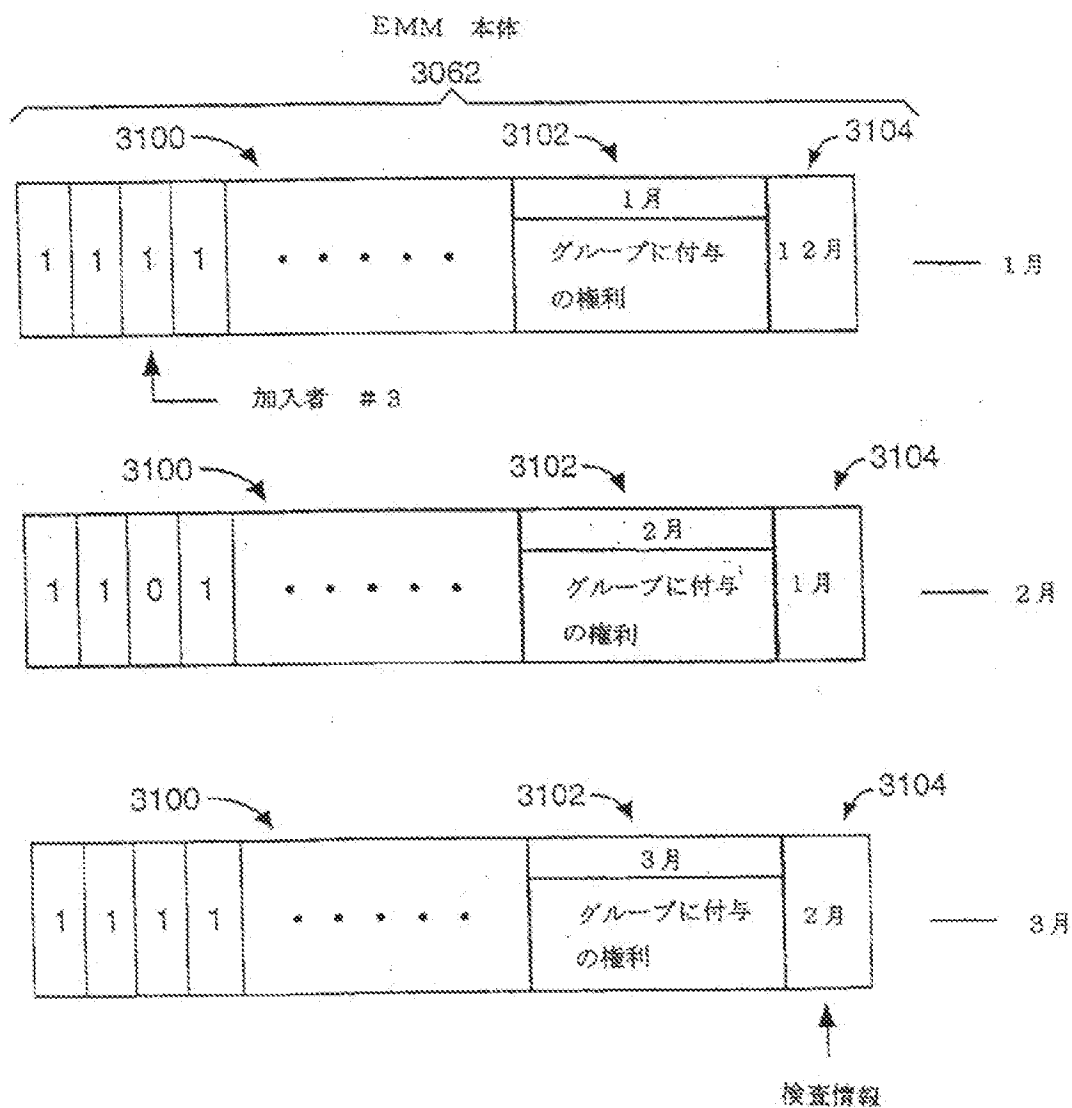


Fig.6.

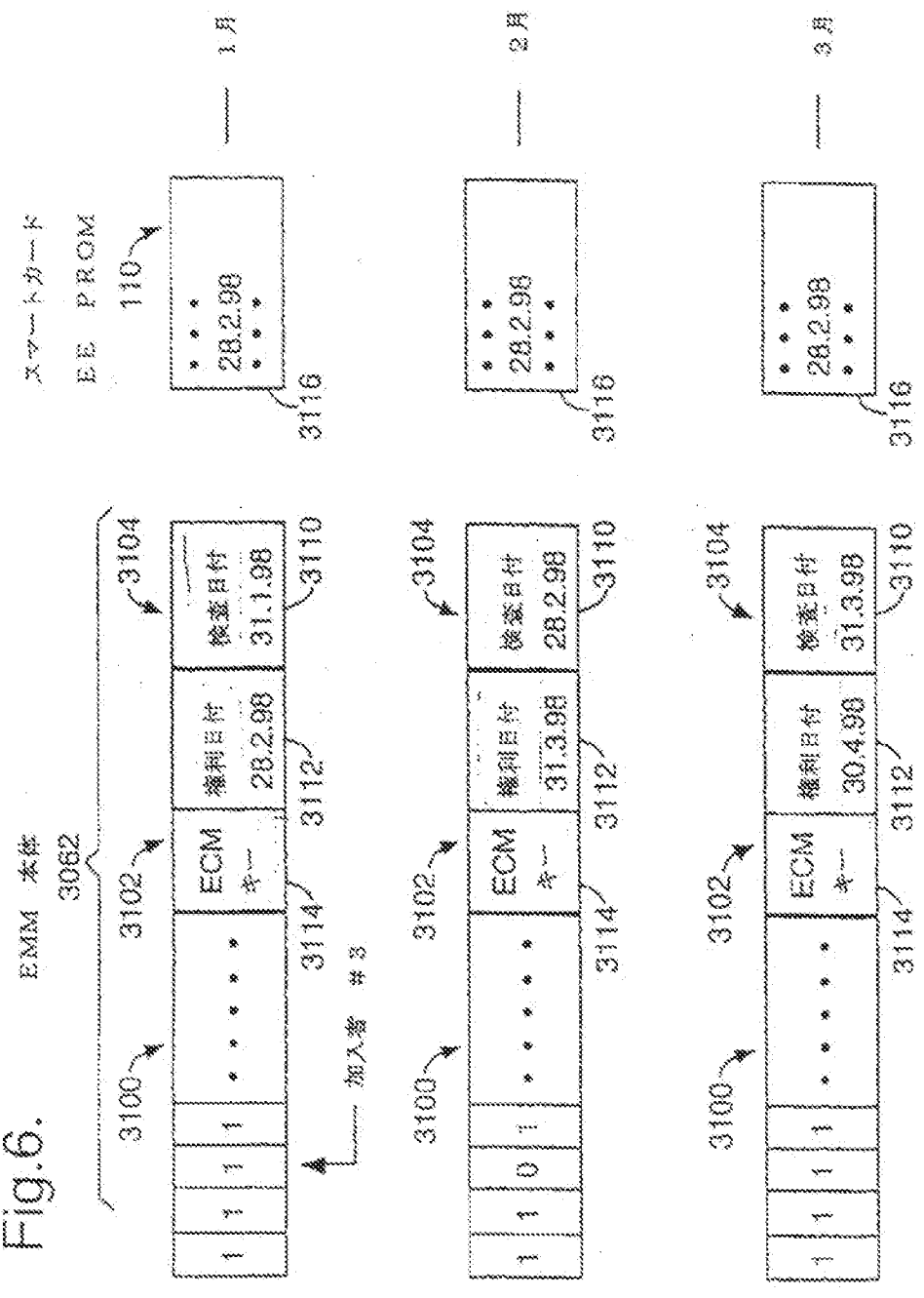




Fig.7.

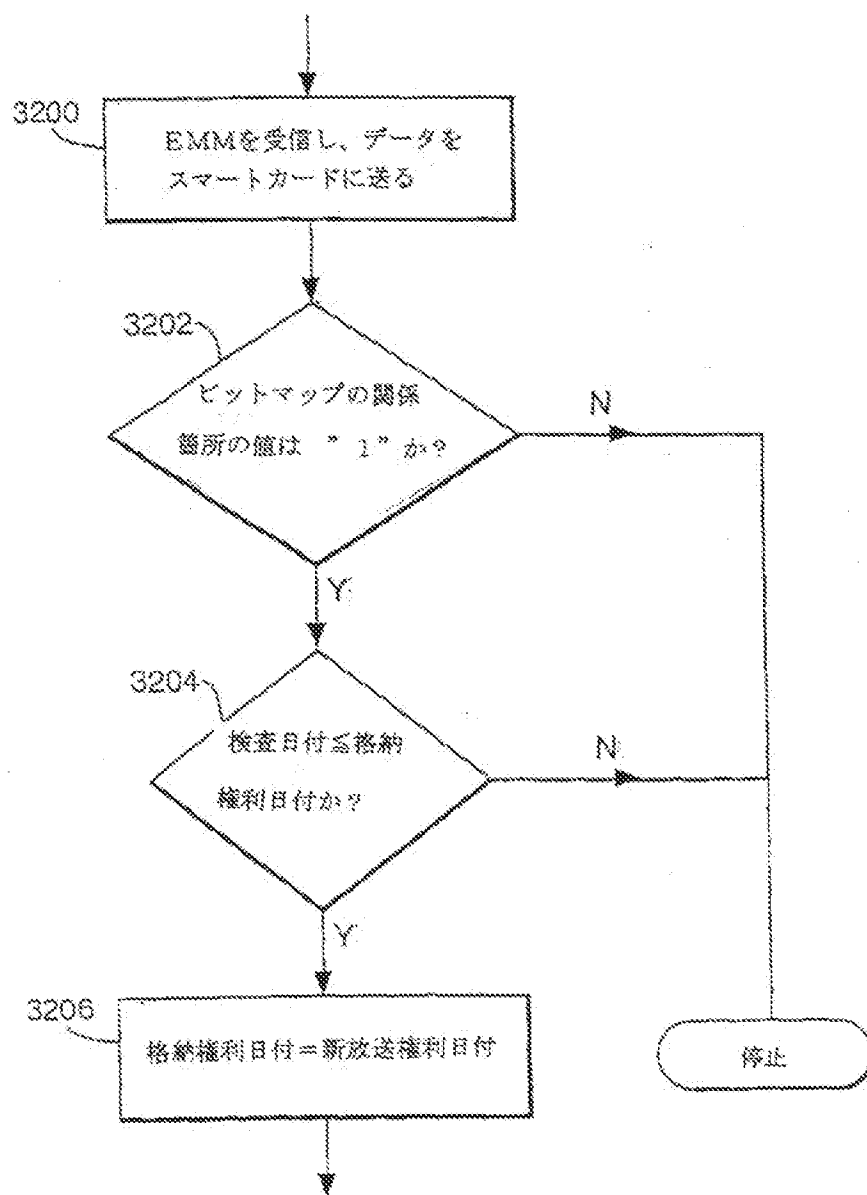
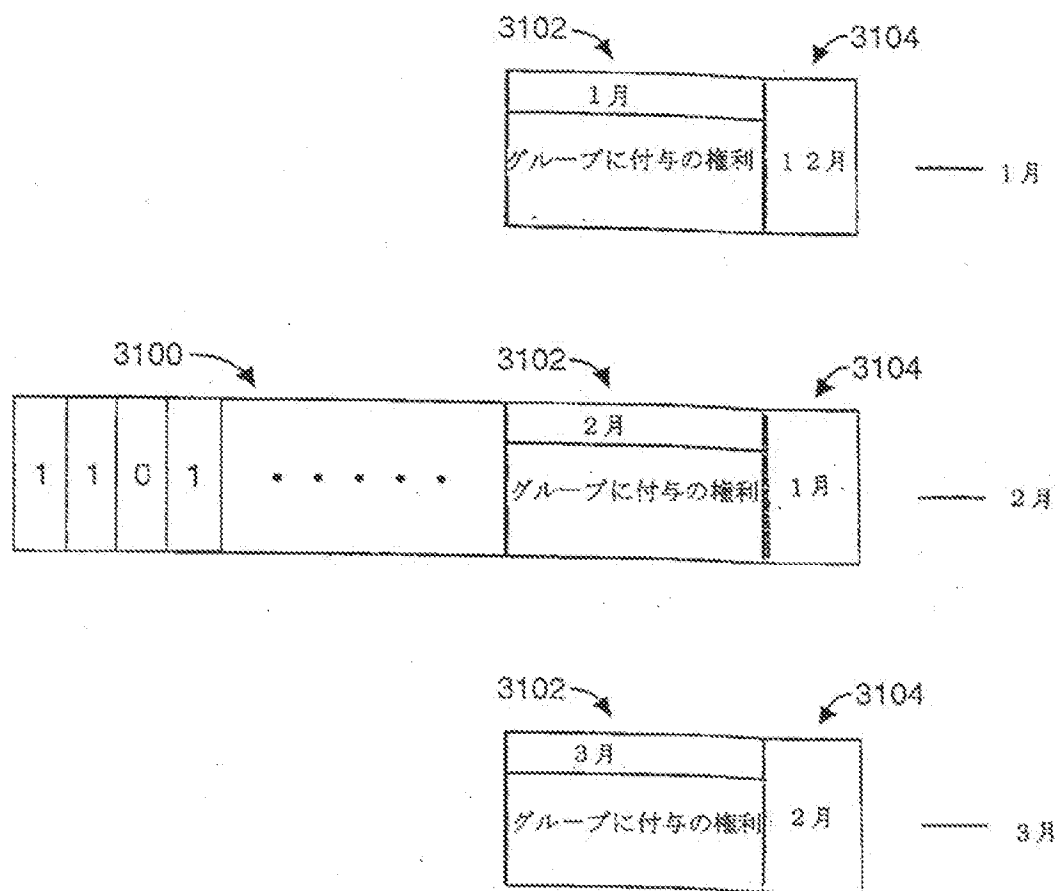


Fig.8.



## INTERNATIONAL SEARCH REPORT

International Application No.

PCT/EP 98/01606

A. CLASSIFICATION OF SUBJECT MATTER  
 IPC 6 H04N7/16 H04N7/167

According to International Patent Classification (IPC) or to other national classification and IPC

## B. FIELDS SEARCHED

Machine documentation searched (classification system followed by classification symbols)

IPC 6 H04N

Documentation searched other than machine documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, patent terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of the relevant passages	Relevant to claim no.
A	EP 0 762 936 A (LG ELECTRONICS INC) 19 March 1997 see column 16, line 9 - line 46 see column 24, line 18 - column 25, line 37	1-17
A	WO 85 00718 A (INDEP BROADCASTING AUTHORITY) 14 February 1985 see page 3, line 30 - page 4, line 4 see page 7, line 23 - line 35 see page 11, line 1 - page 12, line 15	1-17

-/-



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

## \* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to underpin the principal or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be recognized to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"Z" document member of the same patent family

Date of the actual completion of the international search

30 July 1998

Date of ending of the international search report

07/08/1998

Name and mailing address of the ISA

European Patent Office, P.O. Box 5818, Finkenstr. 2  
 NL - 2280 HW Rijswijk  
 Tel: (+31-70) 340-2040, Tx: 31 851 490 01,  
 Fax: (+31-70) 340-9016

Authorizing officer

Poirier, J-M

## INTERNATIONAL SEARCH REPORT

national Application No.

PCT/EP 98/01606

C (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication where appropriate, of the relevant passages	Relevant to claim No.
A	WO 96 06504 A (CHANEY JOHN WILLIAM (THOMSON CONSUMER ELECTRONICS (US)) 29 February 1996 see page 2, line 11 - line 33 see page 6, line 11 - line 24 see page 10, line 3 - line 12 see page 20, line 8 - line 28 -----	1-17
A	WO 96 29560 A (THOMSON CONSUMER ELECTRONICS) 2 November 1996 see page 7, line 17 - page 8, line 32 -----	1-17
P, A	EP 0 817 485 A (THOMSON MULTIMEDIA SA) 7 January 1998 see the whole document -----	1-17
A	EP 0 153 837 A (MATSUSHITA ELECTRIC IND CO LTD) 4 September 1985 see page 4, line 22 - page 5, line 8 -----	1
A	WO 97 04553 A (PHILIPS ELECTRONICS NV (PHILIPS NORDEN AB (SE)) 6 February 1997 -----	
A	EP 0 723 371 A (THOMSON MULTIMEDIA SA) 24 July 1996 -----	

Form PCT/IS 4242 (continuation of a search sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No.

PCT/EP 98/01606

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0763936 A	19-03-1997	CN 1150738 A	28-05-1997
		JP 9093561 A	04-04-1997
WO 8500718 A	14-02-1985	DE 3470646 A	26-05-1988
		DE 3474496 A	10-11-1988
		EP 0151147 A	14-08-1985
		EP 0148235 A	17-07-1985
		WO 8500491 A	31-01-1985
		JP 5025436 B	12-04-1993
		JP 60501882 T	31-10-1985
		US 4736422 A	05-04-1988
		US 4802215 A	31-01-1989
WO 9606504 A	29-02-1996	AU 3238598 A	22-03-1996
		AU 3239495 A	14-03-1996
		BR 9508621 A	30-09-1997
		CA 2196405 A	07-03-1996
		CA 2196407 A	29-02-1996
		CN 1158202 A	27-08-1997
		CN 1158203 A	27-08-1997
		EP 0782807 A	09-07-1997
		FI 970677 A	18-02-1997
		JP 10506507 T	23-06-1998
		JP 10506720 T	02-06-1998
		PL 318647 A	07-07-1997
		WO 9607267 A	07-03-1996
WO 9529560 A	02-11-1995	US 5619501 A	08-04-1997
		CA 2188127 A	02-11-1995
		CN 1151233 A	04-06-1997
		CN 1167405 A	10-12-1997
		EP 0756801 A	05-02-1997
		JP 9512675 T	16-12-1997
EP 0817485 A	07-01-1998	FR 2750554 A	02-01-1998
		CN 1171015 A	21-01-1998
		JP 10164052 A	19-06-1998
EP 0163837 A	04-09-1985	JP 1866645 C	26-08-1994
		JP 60171880 A	05-09-1985

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No.

PCT/EP 98/01606

Patent document cited in search report	Publication date	Patent family members	Publication date
EP 0153837 A		JP 1734515 C	17-02-1993
		JP 4020316 B	02-04-1992
		JP 60171885 A	05-09-1985
		JP 1734516 C	17-02-1993
		JP 4020317 B	02-04-1992
		JP 60171886 A	05-09-1985
		JP 1866647 C	26-08-1994
		JP 60171893 A	05-09-1985
		AU 559311 B	05-03-1987
		AU 3864285 A	22-08-1985
		CA 1278855 A	08-01-1991
		DE 3584575 A	12-12-1991
		US 4833710 A	23-05-1989
WO 9704553 A	06-02-1997	EP 0793880 A	10-02-1997
		JP 10505995 T	09-06-1998
EP 0723371 A	24-07-1996	FR 2729521 A	19-07-1996
		JP 8307850 A	22-11-1996

(31)優先権主張番号 97402959.7

(32)優先日 平成9年12月5日(1997.12.5)

(33)優先権主張国 ヨーロッパ特許庁(EP)

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW